

BUTLER | SNOW

March 17, 2023

VIA ELECTRONIC FILING

Electronically Filed in TPUC Docket
Room on March 16, 2023 at 2:37 p.m.

Hon. Herbert H. Hilliard, Chairman
c/o Ectory Lawless, Docket Room Manager
Tennessee Public Utility Commission
502 Deaderick Street, 4th Floor
Nashville, TN 37243
TPUC.DocketRoom@tn.gov

RE: *Rulemaking to Promulgate Rules for Utility Cybersecurity Plan Reporting as Required Under Tenn. Code Ann. § 65-4-127, TPUC Docket No. 23-00001*

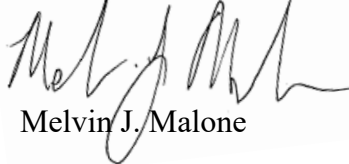
Dear Chairman Hilliard:

Please find attached for filing *Comments of Tennessee American Water Company in Response to Notice of Open Docket for Filing Comments* in the above-captioned docket.

As required, the original plus four (4) hard copies will be mailed to your office. Should you have any questions concerning this filing, or require additional information, please do not hesitate to contact me.

Very truly yours,

BUTLER SNOW LLP



Melvin J. Malone

clw

Attachment

cc: Bob Lane, TAWC

Erik Lybeck (Atmos Energy Corporation)
Paul S. Davidson (Piedmont Natural Gas Company, Inc.)
J. W. Luna (Chattanooga Gas Company)
Floyd R. Self (Chattanooga Gas Company)
Vance Broemel, Consumer Advocate
Karen Stachowski, Consumer Advocate

*The Pinnacle at Symphony Place
150 3rd Avenue South, Suite 1600
Nashville, TN 37201*

MELVIN J. MALONE
615.651.6705
melvin.malone@butlersnow.com

T 615.651.6700
F 615.651.6701
www.butlersnow.com

BUTLER SNOW LLP

**BEFORE THE TENNESSEE PUBLIC UTILITY COMMISSION
NASHVILLE, TENNESSEE**

IN RE:)	
)	
RULEMAKING TO PROMULGATE)	
RULES FOR UTILITY)	DOCKET NO. 23-00001
CYBERSECURITY PLAN REPORTING)	
AAS REQUIRED UNDER TENN CODE)	
SECTION 65-4-127)	

**COMMENTS OF TENNESSEE AMERICAN WATER COMPANY
IN RESPONSE TO NOTICE OF OPEN DOCKET FOR FILING COMMENTS**

Tennessee American Water Company (“TAWC” or “Company”) respectfully submits the Comments of Tennessee American Water Company in Response to the Notice of Open Docket for Filing Comments in *In Re: Rulemaking to Promulgate Rules for Utility Cybersecurity Plan Reporting as Required under Tenn. Code Ann Section 65-4-127*, TPUC Docket No. 23-00001. TAWC appreciates and values the opportunity to participate in this rulemaking and to submit comments on this essential critical subject.

TAWC is a public utility engaged in the provision of water in the State of Tennessee and is subject to the jurisdiction of the Tennessee Public Utility Commission (“Commission” or “TPUC”). Thus, TAWC would be subject to the rules that emanate from this rulemaking proceeding.

TAWC respectfully requests that any parties filing comments or other pleadings in this docket kindly provide a copy to the following representatives of the Company:

Melvin J. Malone, Esq
Butler Snow LLP
150 3rd Avenue South, Suite 1600
Nashville, TN 37201
Telephone: (615)651-6705
Melvin.malone@butlersnow.com

David L. Pippen
Sr Director – Corporate Counsel
Tennessee and Kentucky American Water
2300 Richmond Road
Lexington, KY 46143
Telephone: (317)-807-2460
David.pippen@amwater.com

Bob Lane
Sr. Manager Rates and Regulation
Tennessee American Water
109 Wiehl Street
Chattanooga, TN 37408
Telephone (423)771-4795
bob.lane@amwater.com

TAWC firmly believes that cybersecurity is a critical element in today's global environment to ensure reliable, safe, and clean water and to protect the data and information of our customers and the utility. Therefore, support both the Tennessee General Assembly's and the Commission's intention to have all utilities subject to Tenn. Code Ann. § 65-4-127 to have in place a cybersecurity plan. TAWC respectfully submits the following comments.

I.

BACKGROUND

On June 1, 2022, Public Chapter 1111 concerning utility cybersecurity plans was signed into law. The sections of Public Chapter 1111 relating to the Tennessee Public Utility Commission are codified in Tenn. Code Ann. § 65-4-127. The statute requires that “a utility shall prepare and implement a cybersecurity plan to provide for the protection of the utility's facilities from

unauthorized use, alteration, ransom, or destruction of electronic data.”¹ Further, the statute provides that subject utilities shall annually submit documentation of the utility's compliance with this statute to the Commission by July 1. To address new threats, the law requires each utility to “assess and update the cybersecurity plan implemented pursuant to this no less frequently than every two years to address new threats.”²

TAWC supports the promulgation of rules requiring that utilities develop or have in place a cybersecurity plan to provide for the protection of the utility’s facilities from unauthorized use, alteration, ransom, or destruction of electronic data. TAWC, its parent and its affiliated companies have operations in 13 states and provides cybersecurity across the company for Information Technology System or Operational Technology system. TAWC is a subsidiary of American Water, the largest investor-owned water and wastewater utility in North America. In addition to our water and wastewater regulated public utilities, the Company’s affiliates provide water and wastewater service to the US military through our Military Services Group. Due to our size and reach, our cybersecurity investment and plans are made at a national level and any state regulation should be general and flexible enough to harmonize with federal level cybersecurity law, regulation, and guidance, as well as those of other security agencies and states. The Company, its parent and its affiliated companies have invested and will continue to invest considerable resources and effort in developing and maintaining robust and effective cybersecurity protections and plans.

TAWC urges that the Commission’s cybersecurity rules are developed to be general in nature, as the utilities it regulates that are subject to these rules span several utility sectors. Additionally, many utilities subject to the Commission’s jurisdiction, including TAWC, operate in multiple jurisdictions, operate under the umbrellas of a holding company, and have parent and

¹ § 65-4-127 (b)(1)

² § 65-4-127 (b)(2)(c)

affiliated companies. Broad rules, focusing on the mandate from the legislature to ensure that utilities have a security plan in place and implemented, will allow TAWC and other utilities subject to these rules to optimize security plans to best fit its respective sector specific needs, security concerns and legal framework.

The United States Environmental Protection Agency (“EPA”) has been designated by the Department of Homeland Security as the Sector Risk Management Agency for the Water and Wastewater Systems. In this role, the EPA has promulgated requirements and guidelines governing cybersecurity at the nation’s water and wastewater systems. For example, on March 3, 2023, the EPA issued a directive under which states must evaluate the cybersecurity of operational technology used by a public water system (PWS) when conducting a PWS sanitary survey or through other state programs.

The Commission’s rules should be broad enough and flexible enough complement rules and guidelines established by other agencies also charged with the responsibility for the cybersecurity of water and wastewater utilities.

The cybersecurity stance of TAWC and other utilities must be adaptive enough to react to emerging threats. Cyber threats are dynamic in nature and utilities cyber plans must be adaptive enough to respond accordingly. Additionally, the Commission must be aware of the serious sensitivity of cybersecurity information and the risks inadvertent or other disclosures creates. With a few minor changes, the Commission proposed rules can meet the objectives of the legislature, the Commission, and the utilities to protect against cyber threats.

II.

COMMENTS

The Commission’s proposed cybersecurity rules focus on three (3) separate components:

- 1) requiring all jurisdictional utilities have in place or prepare and implement a cybersecurity plan and file an annual self-certification form that such a plan is in place and reviewed at least every two years;
- 2) requiring those utilities have a plan for communicating a cybersecurity event; and
- 3) a requirement to report a “cybersecurity event” to the Commission.

Only the first of the above-referenced three (3) components is required by the statute. For this reason, and consistent with the intent of the Tennessee General Assembly, TAWC suggests that the Commission focus on rules on ensuring that the utilities under its jurisdiction have in place a cybersecurity plan.

TAWC has the following specific concerns with the proposed rules.

1. Cybersecurity Plan: Section 122-4-15-.03(1)

TAWC supports the promulgation of rules requiring that utilities develop or have in place a cybersecurity plan to provide for the protection of the utility facilities from unauthorized use, alteration, ransom, or destruction of electronic data. This requirement fulfils a requirement of Public Chapter 1111 relating to the Tennessee Public Utilities Commission as codified in Tennessee Code Annotated § 65-4-127.

2. Cybersecurity Plan: Section 122-4-15-.03(2)

TAWC supports the requirement that a utility periodically review their cybersecurity plan and supports the minimum two-year timeframe for this review and, if needed update, to the plan. Cybersecurity is a dynamic landscape with new threats and threat vectors that must be protected against. Ongoing review and updating is essential in such an environment.

3. Annual Filing Requirements: Section 122—4-15-.04(1)(a.)

The proposed rules call for the submittal of a “summary of the program and procedures that describe the utilities approach to cybersecurity.” Whenever possible, TAWC minimizes the external sharing of highly confidential information and confidential security information, thus this proposal raises concerns for TAWC. First the applicable statute does not require such a summary. Second TAWC is concerned about the potential security issues raised by even the most high-level summary of a program. Cybersecurity information is among the most sensitive and confidential information the utility has and it is not shared lightly. Third, the TPUC must ensure that any data provided to it is at a minimum handled by the Commission must be in compliance with any laws, rules and regulations governing sensitive security information. For example, the TSA has rules governing the treatment of “Sensitive Security Information” and how it must be protected.³ Such laws, rules and regulations may be instituted by for the Water and Waste-water sector in the future as well. The TPUC should not require the provision of a summary of the plan because 1) is not required by law, 2) raises security concerns, and 3) could place significant information security burdens and risks on the Commission.

4. Annual Filing Requirements: Section 122—4-15-.04(1)(b)

The proposed rules require the attestation to include the contact information of employee(s) responsible for cybersecurity. TAWC believes that requiring this information, provided it is held confidential by the Commission due to its sensitivity, is appropriate.

5. Annual Filing Requirements: Section 122—4-15-.04(1)(c)

TAWC agrees and supports the requirement that cybersecurity plans have a training component. Employees are a company’s strongest asset. However, they are also a company’s

³ 49 CFR parts 15 and 1520.

biggest risk when it comes to cybersecurity. Employees that are trained in cybersecurity awareness are a key component of any cybersecurity program.

6. Annual Filing Requirements: Section 122—4-15-.04(1)(d).

Requires a statement indicating whether the utility has “a plan for communicating a cybersecurity event that results in a loss of service, financial harm or breach of sensitive information.” Requiring notification or other communications of a cyber event is not required by Public Chapter 1111 and as such the Commission should tread cautiously in the area.

First, requiring notification “cybersecurity event” also requires that the Commission undertake the task of defining a “cybersecurity event.” The term cybersecurity event and cybersecurity incident are terms of art in the cybersecurity world. For example, the Cybersecurity and Infrastructure Security Agency uses the term “cyber-incidents.” TAWC suggests that the definition use the term cyber security incident to be more consistent with other cyber security structures.

Water utilities are already required to report such incidents. In March 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (“CIRCI”) was signed into federal law, which requires, among other things, that water utilities and other covered entities report cyber incidents to the Cybersecurity and Infrastructure Security Agency (“CISA”) within 72 hours from when the incident occurred.

In the operation of the rule Commission should not require or expect a detailed description of any “communications plan” as that is very sensitive and too much disclosure could benefit malicious actors.

7. Annual Filing Requirements: Section 122—4-15-.04(1)(e).

Again, TAWC cautions the Commission in its efforts to remain mindful of the extreme sensitive nature of cybersecurity information. This summary is not required by law and therefore is an avoidable risk. TAWC recommends deleting this requirement. However, should the Commission desire to have such summaries provided, the summaries should be afforded the highest level of confidentiality and security the Commission can develop for protecting this information. Particularly, malicious actors could benefit from knowledge about the material impact of a breach or other cybersecurity incident and what mitigating actions had been take.

8. Annual Filing Requirements: Section 122—4-15-.04(1)(f).

This section requires a “statement indicating whether the utility has procured cybersecurity insurance, and, if so, the current term and limits of such coverage.” So long as this information is not made public and is treated as confidential and sensitive, the Company does not object to informing the Commission in its annual filing whether the utility has procured cybersecurity insurance. However, TAWC does not believe that it is prudent to provide the term and amount. Doing so would create a significant risk for the Company and other utilities subject to this rule. Such information could be, and reportedly has been, used by malicious actors to narrow down targets and to set “ransomware” demand levels. Providing such information to the Commission creates an unnecessary risk to the Company, the Commission, and our customers.

9. Annual Filing Requirements: Section 122—4-15-.04(2)

TAWC supports the requirement that the documentation filed must include a sworn statement by the utility's chief executive officer, president or another person with an equivalent role. However, TAWC suggests this to be broadened to include “or their designee with

cybersecurity oversight and responsibility such as the chief security officer or director of cybersecurity.”

TAWC has no issues with the three (3) components that shall, at a minimum be affirmed: a) has prepared and implemented the cybersecurity plan described in the filing; b) the cybersecurity plan has been prepared or updated with in the past two years, and c) that all documentation and information filed in current and accurate.

10. Required Notification to Commission: 122-4-15-.06

This proposed Rule requiring notification of the Commission Chair within 48 hours of experiencing a “cybersecurity event” is not required by Public Chapter 1111. This gives the Commission flexibility with regard to this rule.

Requiring notification of a “cybersecurity event” also requires that the Commission enter into the task of defining a “cybersecurity event.” The term cybersecurity event and cybersecurity incident are terms of art in the cybersecurity world. For example, the Cybersecurity and Infrastructure Security Agency uses the term “cybersecurity incidents.” TAWC suggests redefining this to be a “cybersecurity incident” to be more consistent with other cybersecurity reporting structures.

Investigations of a potential cybersecurity incident may take considerable time and resources to determine the root cause of the incident. TAWC agrees with Chattanooga Gas that the utilities first reporting obligation is to relevant law enforcement agencies, as well as agencies responsible for supporting and mitigating further damage or intrusion. Additionally, law enforcement may not want immediate disclosures of some incidents to regulators.

In March 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (“CIRCI”) was signed into federal law, which requires, among other things, that water utilities

and other covered entities report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency (“CISA”) within 72 hours from when the incident occurred. To be consistent with this, the proposed rule should be amended to require that a report to the Commission occur within 72 hours after a cybersecurity incident or confirmation that a cyber security incident occurred, whichever is later. Additionally, any reporting by a utility should only be done to the extent allowed by law enforcement or applicable law, rule or regulations.

Section 1220-04-03-.42 already deals with the notification of the Commission for interruptions of service and the cause. This, TAWC believes, would include notification for unplanned interruptions of service resulting from a cybersecurity incident. However, any such reporting should be consistent with these cybersecurity rules, and be consistent with other applicable laws, rules and regulations and not counter to the wishes or demands of law enforcement.

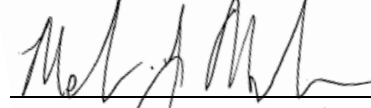
III.

CONCLUSION

TAWC supports the desire of the Tennessee General Assembly, Governor Bill Lee, and the Public Utility Commission in taking steps to ensure that all utilities, including TAWC, have in place a cybersecurity plan and that plan is revisited and reviewed at least every two years. TAWC has such a plan in place. Promulgation of rules requiring that utilities develop or have in place a cybersecurity plan to provide for the protection of the utility facilities from unauthorized use, alteration, ransom, or destruction of electronic data is in the public interest and is necessary for clean, reliable, and safe drinking water. Staying within the expressed framework of the state statute provides the best hope of crafting rules that are effective, not inconsistent with other cybersecurity rules and guidelines and appropriately flexible. For ease of reference, a redlined version of the proposed rules reflecting most, if not all, of TAWC’s comments is attached.

As noted at the outset herein, the Company appreciates and values the opportunity to participate in this rulemaking proceeding and to submit the above-outlined comments.

RESPECTFULLY SUBMITTED,

A handwritten signature in dark ink, appearing to read 'Melvin J. Malone', is written over a horizontal line.

MELVIN J. MALONE (BPR #013874)

Butler Snow LLP

150 3rd Avenue South, Suite 1600

Nashville, TN 37201

melvin.malone@butlersnow.com

(615) 651-6705

Attorneys for Tennessee American Water Company

1220-04-15-.01 Definitions

(1) Commission - means the Tennessee Public Utility Commission.

(2) Cybersecurity ~~event~~ incident - any unauthorized use, alteration, ransom, or destruction of electronic data involving a utility's information or operation technology systems; a cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.

(3) Cybersecurity plan - a plan that provides for the protection of the utility's information technology and operational technology systems from unauthorized use, alteration, ransom, or destruction of electronic data.

(4) Information Technology - any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the utility. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

(5) Information Technology System (IT System) - hardware and software related to electronic processing, and storage, retrieval, transmittal, and manipulation of data.

(6) Operational Technology - programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment) used to provide utility service. These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.

(7) Operational Technology System (OT System) - a system or network that monitors or controls electric, gas, wastewater or water system infrastructure used for utility operations.

(8) Utility - a public utility defined by T.C.A. § 65-4-101 that provides electric, water, wastewater, or natural gas services.

Authority: T.C.A. §§ 65-2-102, 65-4-101, and 65-4-127.

1220-4-15-. 02 Confidentiality

All documentation submitted in accordance with T.C.A. § 65-4-127 and these rules shall be treated as confidential and protected from public inspection. [The Commission shall treat this documentation consistent with any federal laws, regulation or rule that protects sensitive security information or similarly designated information regarding cyber security.](#)

Authority: T.C.A. §§ 65-2-102, 65-4-127, 10-7-504(a)(21)(i), and 10-7-504(a)(21)(C)(iii).

SS-7037 (March 2020) 2 RDA 1693

1220-4-15-.03 Cybersecurity Plan

(1) By July 1, 2023, or within one (1) year after a utility is formed, whichever is later, a utility shall prepare and implement a cybersecurity plan.

(2) Cybersecurity plans implemented in compliance with these rules must be assessed and updated by the utility no less frequently than once every two (2) years to address new threats.

Authority: T.C.A. §§ 65-2-102 and 65-4-127.

1220-4-15-.04 Annual Filing Requirements

(1) By July 1st of each calendar year, all utilities shall submit an attestation that the utility has prepared and implemented a cybersecurity plan. At a minimum, the attestation shall include:

~~(a) A summary of the program and procedures that describe the utility's approach to cybersecurity awareness and protection;~~

~~(b)~~ Contact information for utility employee(s) responsible for cybersecurity;

(c) A statement indicating whether the utility conducts annual cybersecurity training for the utility personnel with access to any utility IT or OT system;

(d) A statement indicating whether the utility has a plan for communicating a cybersecurity event that results in loss of service, financial harm, or breach of sensitive business or customer data. The statement should specify whether the plan includes notification to the Commission and utility customers;

~~(e) A summary of any cybersecurity event during the reporting year that resulted in material loss of service, financial harm, or breach of sensitive business or customer data, including parties notified of the unauthorized action and remedial actions undertaken; and~~

(f) A statement indicating whether the utility has procured cybersecurity insurance , ~~and, if so, the current term and limits of such coverage.~~

(2) The documentation filed must include a sworn statement by the utility's chief executive officer, president or another person with an equivalent role and authority. Such statement shall, at a minimum, affirm that the utility:

(a) Has prepared and implemented the cybersecurity plan described in the filing;

(b) The cybersecurity plan has been prepared or updated within the last two (2) years; and

(c) That all documentation and information filed is current and accurate.

Authority: T.C.A. §§ 65-2-102 and 65-4-127.

1220-4-15-.05 Failure to Comply; Sanctions

(1) A utility fails to comply with these rules, and is considered in non-compliance, when:

(a) The company does not file documentation required by these rules showing that it has prepared a cybersecurity plan by July 1st of each calendar year; and

(b) The company does not file documentation required by these rules showing that it has implemented that cybersecurity plan by July 1st of each calendar year.

(2) After hearing, the Commission may impose reasonable sanctions, including civil and monetary penalties, against a utility in non-compliance with these rules.

(3) Monetary penalties imposed by the Commission will be consistent with the statutory limit set in T.C.A. § 65-4- 120.

(4) If the Commission determines that sanctions shall include a monetary penalty, it may consider:

SS-7037 (March 2020) 3 RDA 1693

(a) The efforts the utility to comply with these rules;

(b) The financial stability of the utility; and

(c) The impact of noncompliance on customers of the utility.

(5) The Commission may require a utility to establish a separate fund to further support its compliance with these rules.

(6) Any utility in non-compliance shall be reported to the General Assembly in accordance with TC.A § 65-4-127(f).

Authority: TC.A §§ 65-2-102, 65-4-120, and 65-4-127.

1220-4-15-.06 Required Notification to Commission of Cyber Event

(1) If a utility experiences a cybersecurity ~~event~~incident, it shall notify to the extent allowed by law, regulation or rule and permitted by law enforcement, both verbally and in writing, the Chair of the

Commission or their designee within ~~48-72~~ hours of the utility's discovery of the cybersecurity event or confirmation of a cyber incident, whichever is later.

(2) Within 30 days of the discovery or confirmation of the cybersecurity ~~event~~incident, the utility shall be available and prepared to brief the Chair of the Commission or their designee on the impact of the cybersecurity event to utility customers and on utility operations.

Authority: TC.A §§ 65-2-102 and 65-4-127.

1220-4-15-.07 Cost Recovery for Cybersecurity Investment

(1) To the extent that costs related to action required by this rule are not already recovered in rates, the utility may seek cost recovery:

(a) By filing a petition pursuant to TC.A 65-5-103; or

(b) If permissible, by requesting an alternative regulatory mechanism pursuant to TC.A. 65-5-103(d).

Authority: TC.A §§ 65-2-102, 65-4-127, and 65-5-103.

SS-